the local government's civil service selection procedures.

[59 FR 36089, July 15, 1994, as amended at 60 FR 29500, June 5, 1995]

237.7402 Contract clause.

Use the clause at 252.237–7022, Services at Installations Being Closed, in solicitations and contracts based upon the authority of this subpart.

[59 FR 36089, July 15, 1994, as amended at 60 FR 29500, June 5, 1995]

PART 239—ACQUISITION OF INFORMATION TECHNOLOGY

Subpart 239.1—General

Sec.
239.101 Policy.

Subpart 239.70—Exchange or Sale of Information Technology

239.7001 Policy.

Subpart 239.71—Security and Privacy for Computer Systems

239.7100 Scope of subpart.
239.7101 Definition.
239.7102 Policy and responsibilities.
239.7102–1 General.
239.7102–2 Compromising emanations—TEMPEST or other standard.
239.7103 Contract clause.

Subpart 239.72—Standards

239.7201 Solicitation requirements.

Subpart 239.73 [Reserved]

Subpart 239.74—Telecommunications Services

239.7400 Scope.
239.7401 Definitions.
239.7402 Policy.
239.7403–239.7404 [Reserved]
239.7405 Delegated authority for telecommunications resources.
239.7406 Cost or pricing data and information other than cost or pricing data.
239.7407 Type of contract.
239.7408 Special construction.
239.7408–1 General.
239.7408–2 Applicability of construction labor standards for special construction.
239.7409 Special assembly.
239.7410 Cancellation and termination.
239.7411 Contract clauses.

AUTHORITY: 41 U.S.C. 421 and 48 CFR chapter 1.

SOURCE: 56 FR 36429, July 31, 1991, unless otherwise noted.

Subpart 239.1—General

239.101 Policy.

See Subpart 208.74 when acquiring commercial software or software maintenance.

[67 FR 65512, Oct. 25, 2002]

Subpart 239.70—Exchange or Sale of Information Technology

239.7001 Policy.

Agencies shall follow the procedures in DoD 4140.1–R, DoD Supply Chain Materiel Management Regulation, Chapter 9, Section C9.5, when considering the exchange or sale of Government-owned information technology.

[71 FR 39010, July 11, 2006]

Subpart 239.71—Security and Privacy for Computer Systems

SOURCE: 69 FR 35534, June 25, 2004, unless otherwise noted.

239.7100 Scope of subpart.

This subpart includes information assurance and Privacy Act considerations. Information assurance requirements are in addition to provisions concerning protection of privacy of individuals (see FAR Subpart 24.1).

239.7101 Definition.

Information assurance, as used in this subpart, means measures that protect and defend information, that is entered, processed, transmitted, stored, retrieved, displayed, or destroyed, and information systems, by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

239.7102 Policy and responsibilities.

239.7102–1 General.

(a) Agencies shall ensure that information assurance is provided for information technology in accordance with

current policies, procedures, and statutes, to include—

(1) The National Security Act;

(2) The Clinger-Cohen Act;

(3) National Security Telecommunications and Information Systems Security Policy No. 11;

(4) Federal Information Processing Standards;

(5) DoD Directive 8500.1, Information Assurance; and

(6) DoD Instruction 8500.2, Information Assurance Implementation.

(b) For all acquisitions, the requiring activity is responsible for providing to the contracting officer—

(1) Statements of work, specifications, or statements of objectives that meet information assurance requirements as specified in paragraph (a) of this subsection;

(2) Inspection and acceptance contract requirements; and

(3) A determination as to whether the information technology requires protection against compromising emanations.

239.7102–2 Compromising emanations—TEMPEST or other standard.

For acquisitions requiring information assurance against compromising emanations, the requiring activity is responsible for providing to the contracting officer—

(a) The required protections, *i.e.*, an established National TEMPEST standard (*e.g.*, NACSEM 5100, NACSIM 5100A) or a standard used by other authority;

(b) The required identification markings to include markings for TEMPEST or other standard, certified equipment (especially if to be reused);

(c) Inspection and acceptance requirements addressing the validation of compliance with TEMPEST or other standards; and

(d) A date through which the accreditation is considered current for purposes of the proposed contract.

239.7103 Contract clause.

Use the clause at 252.239–7000, Protection Against Compromising Emanations, in solicitations and contracts involving information technology that requires protection against compromising emanations.

Subpart 239.72—Standards

239.7201 Solicitation requirements.

Contracting officers shall ensure that all applicable Federal Information Processing Standards are incorporated into solicitations.

[71 FR 39011, July 11, 2006]

Subpart 239.73 [Reserved]

Subpart 239.74—Telecommunications Services

239.7400 Scope.

This subpart prescribes policy and procedures for acquisition of telecommunications services and maintenance of telecommunications security. Telecommunications services meet the definition of information technology.

[62 FR 1060, Jan. 8, 1997, as amended at 71 FR 39011, July 11, 2006]

239.7401 Definitions.

As used in this subpart—

(a) *Common carrier* means any entity engaged in the business of providing telecommunications services which are regulated by the Federal Communications Commission or other governmental body.

(b) *Foreign carrier* means any person, partnership, association, joint-stock company, trust, governmental body, or corporation not subject to regulation by a U.S. governmental regulatory body and not doing business as a citizen of the United States, providing telecommunications services outside the territorial limits of the United States.

(c) *Governmental regulatory body* means the Federal Communications Commission, any statewide regulatory body, or any body with less than statewide jurisdiction when operating under the State authority. The following are not ''governmental regulatory bodies''—

(1) Regulatory bodies whose decisions are not subject to judicial appeal; and

(2) Regulatory bodies which regulate a company owned by the same entity which creates the regulatory body.